

how can I comprehensively control sensitive content within Microsoft SharePoint?

agility
made possible™



+

CA Information Lifecycle Control for SharePoint discovers, classifies and controls sensitive information posted, stored and distributed within SharePoint environments. This enables critical business processes to continue while protecting sensitive corporate assets.

+

executive summary

Challenge

Microsoft SharePoint has witnessed significant growth in recent years through the wide adoption of its content management, collaboration and social networking capabilities. But the ease with which SharePoint instances can be deployed has enabled cross functional groups to quickly and sometimes hastily standup instances across the organization. A lack of SharePoint management, design and process has resulted in not only a large volume of SharePoint instances deployed enterprise wide but the growth and exposure of sensitive data. CA DataMinder™ is strategically placed within SharePoint in order to enable business process efficiency to continue while helping to control sensitive information.

Opportunity

Even though SharePoint deployments and the unstructured data contained within containers can often be difficult to manage and secure, there is an opportunity for the business to benefit from the intended uses of SharePoint while also comprehensively protecting the organization from sensitive information compromise. CA DataMinder accomplishes this by taking a risk-based security approach by controlling information throughout the SharePoint information lifecycle. As information is created, stored, revised and distributed within SharePoint, CA DataMinder is able to discover, classify and control sensitive content in order to reduce the risk of information compromise and non-compliance all while enabling business processes to continue.

Benefits

CA Information Lifecycle Control for SharePoint allows organizations to benefit in the following ways:

- Improve effectiveness of measuring information risk through automatic discovery and classification
- Business process enablement while controlling sensitive information throughout the SharePoint information lifecycle
- Reduced risk of information compromise and regulatory non-compliance

Section 1: Challenge

SharePoint usages and challenges

The most critical information challenges organizations are faced with when dealing with SharePoint are often the result of its core capabilities.

Common SharePoint usages

The core function of SharePoint is its ability to store documents and images while acting as a centralized location to collaborate and improve business efficiencies. While it can both centralize information and applications for internal corporate usage it also can provide a forum for partners and 3rd parties to improve business processes and information sharing across organizational boundaries.

But it is these same core functions that can also result in the exposure and compromise of sensitive content (***Intellectual Property, Personally Identifiable Information, Non-Public Information or Protected Health Information***). Users may manually post sensitive content or edit and revise existing content resulting in its increased sensitivity. This typical data usage process can expose organizations to sensitive information compromise with little to no controls to protect the organization.

Posting of information. Users often leverage SharePoint as a repository for storing sensitive documentation and content. But quite often a lack of defined processes or data architecture design enables the posting of sensitive content to the wrong locations or containers. The result is sensitive information being stored within unsuitable locations with little organizational or administrative knowledge.

For example, a finance department may have setup a SharePoint instance with subfolders to store sensitive financial documents such as customer billing and corporate financial information.

- The intent of the data architecture was to create separate containers for specific purposes and organizational functions.
- If the wrong data, such as corporate financial statements, were to be uploaded, posted or moved to an unintended location, such as customer billing, the organization could be at a significant risk of data compromise with a direct financial impact on the business.
- A lack of data management processes often results in the comingling of content across containers unbeknownst to IT, Security or the Information Owners putting the organization at significant risk.

Content collaboration. Collaboration within SharePoint has remained its most popular usage but is also a significant factor in SharePoint information sprawl. Even though SharePoint usage improves communication and business process efficiency it also increases the risk of exposing sensitive corporate information. While the original posting of content could at first be non-impactful to the business, the evolutionary process of content access, collaboration and sharing often results in the appending or net new creation of sensitive information. Access management policies that were originally intended to allow access to non-sensitive information often become outdated and ineffective due to the new forms content takes as collaborative usage occurs.

For example, a company outsourcing core business functions to a business process consulting company collaborates through an integrated SharePoint deployment.

- At first no sensitive information is shared between parties as expected.
- But during the normal process of sharing information an employee appends intellectual property to a document in a manner that doesn't comply with corporate policy.
- Even though defined processes were followed to share information within a properly architected SharePoint environment the company is exposed as a byproduct of collaboration.

Content distribution. Once document collaboration is complete the final copy is often ready for distribution over a variety of communication modes. This often results in sensitive content being copied to storage devices, sent over email, uploaded to social networking sites, transported over mobile devices or even migrated to the cloud. This replication of content significantly increases the exposure level to the business. The accidental, malicious and negligent distribution of content must be controlled in order to reduce the impact to the business.

For example, a business line owner and her direct reports finalize a three year strategy document.

- The business line owner downloads the document locally to her laptop in order to send via email to her general manager.
- But in the process of sending the document she mistakenly types in the wrong email address and accidentally sends the document to an individual outside the company that happens to be a business partner that works with several competitors.
- The mistake is costly but not uncommon. Controls need to be put in place in order to control sensitive information from being sent to unintended recipients as a result of human error.

Challenges with securing SharePoint

The implications of enabling sensitive information to be stored, shared and ultimately exposed within SharePoint results in various challenges that must be dealt with in order to reduce organizational information risks.

Inability to locate information. The same lack of design and process that results in sensitive information exposure within SharePoint also contributes to a lack of visibility and administrative knowledge. Information that doesn't follow pre-defined data architecture designs and segmentation strategies over time will likely end up in unintended locations.

As a result sensitive data ends up spread within and across SharePoint instances as well as distributed inside and outside the organization unknown to administrators and information owners. With limited visibility and knowledge of where information is coming from, where it resides and where it's being moved, security and compliance risk levels can increase significantly often unknown to the organization.

For years organizations have attempted to understand the impact of sensitive information through manual risk assessments delivered on a system by system basis. These assessments, of course, quickly become irrelevant given the dynamic nature of data, making the results stale and close to unusable.

This lack of real-time visibility when data is at-rest, in-use and in-motion can often distort an organization's views of organizational data sensitivity resulting in uninformed IT and security decisions and increased risk levels.

Lack of classification knowledge. Not understanding where sensitive information resides or is communicated directly impacts the ability to assess organizational risk. Businesses often make assumptions on the sensitivity level of content based on where they think information is stored ultimately leaving them with an inaccurate picture.

Organizations must be able to actively classify dynamic information in relation to corporate and regulatory policies in order to accurately measure SharePoint risk levels and prioritize effective security controls. The inability to do so often leave organizations, sometimes blindly, exposed to financial and regulatory risk.

Ineffective information controls. The dynamic nature of data within SharePoint directly impacts an organization's ability to understand where data is, how sensitive data is and the organizations ability to enforce policy and control data. The following depicts the various ways information flows throughout SharePoint, often going unmonitored or controlled.

- **Posting.** Information often starts off sensitive from day one of its creation. A lack of SharePoint control in how information is posted allows sensitive information to easily be uploaded for future access.
- **Storage.** SharePoint data architecture design has the intent of storing information in specific containers to ensure only specific roles and groups can access it. But a lack of entitlement management or data management processes often results in sensitive content being stored in the wrong containers. And regardless of proper architecture design and entitlement management there is sensitive information that should not be stored within SharePoint at any time. Data at this level of sensitivity should be removed or disposed of all together.
- **Access.** Even with the best architecture design and data management processes the collaborative nature of SharePoint enables the creation of sensitive content within the wrong containers. As a result unintended users have access to sensitive content.
- **Distribution.** Once sensitive content is no longer being collaborated on and is in its final state there is little control SharePoint has once the user has downloaded the file to distribute it. The result is sensitive information being exposed through various modes of communication as a result of accidental, negligent or malicious actions.

Section 2: Opportunity

CA Information Lifecycle Control for SharePoint

CA Technologies helps solve the SharePoint information challenges outlined above with SharePoint Information Lifecycle Control. Through automated data discovery, classification and content control, organizations are able to mitigate the risk of information compromise and the financial and regulatory risks that result.

How CA Information Lifecycle Control for SharePoint works

CA Technologies is able to control sensitive information throughout the entire SharePoint Information Lifecycle. Data can now be stored in the right location and accessed, revised and distributed between the right people.

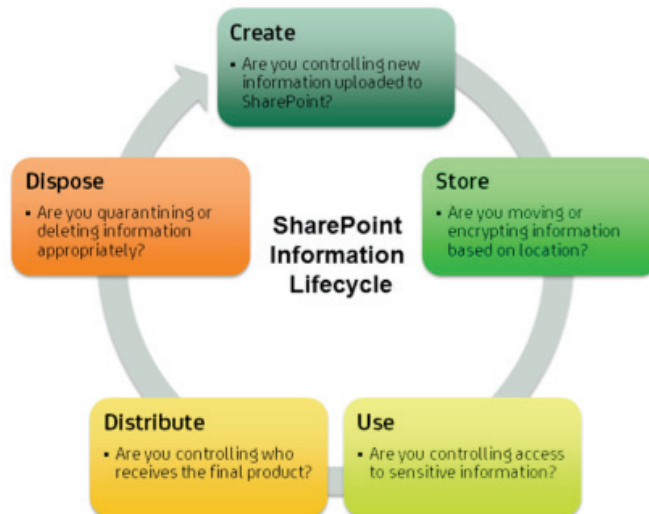
The following depicts how CA DataMinder controls sensitive content throughout the SharePoint Information Lifecycle:

- 1. Create.** Are you controlling information uploaded to SharePoint?
CA DataMinder™ Endpoint controls information uploaded to SharePoint based on its sensitivity and the identity of the user. This prevents extremely sensitive information from being stored and shared within SharePoint while mitigating the risk of unintended users gaining access and compromising it.
- 2. Store.** Are you moving or encrypting information based on location and sensitivity?
CA DataMinder™ Stored Data controls information once it's stored within SharePoint. If sensitive information is located in the incorrect folder CA DataMinder is able to move it. If sensitive information is stored in the clear and requires encryption protection CA DataMinder is able to encrypt it.
- 3. Use.** Are you controlling access to sensitive information?
CA DataMinder is also able to provide third-party technologies, such as web access management products including CA SiteMinder® Classification, information to make fine-grained access decisions. Access can be blocked if users attempting to access information within SharePoint should not be accessing certain content due to their role.
- 4. Distribute.** Are you controlling who receives the final document?
CA DataMinder Endpoint or CA DataMinder™ Email is able to control the distribution of information through a wide range of communications including email, webmail, social media, removable media and printing. It's able to control the distribution of information by warning, encrypting, quarantining and blocking.
- 5. Dispose.** Are you quarantining or deleting sensitive information?

In addition to CA DataMinder Stored Data moving or encrypting data at-rest it's able to remove sensitive information that shouldn't be stored within SharePoint.

Figure A.

CA Information Lifecycle Control for Sharepoint.



Section 3: Use cases

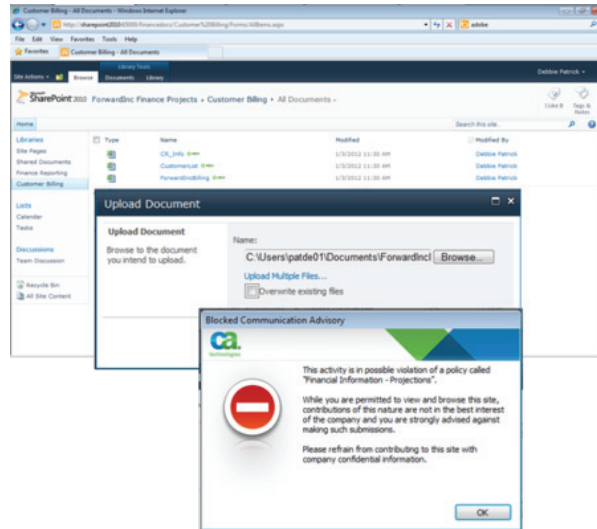
CA DataMinder SharePoint use cases

The following depicts how CA DataMinder controls sensitive content attempting to be posted:

1. A financial controller creates a new spreadsheet containing corporate forecasting information locally to his workstation.
2. Sensitive information can range from payroll data, social security numbers, health or medical records, intellectual property or non-public information but in this scenario it is financially related.
3. This information is tightly controlled and should only be stored within certain SharePoint containers in order to protect the business from leaking information prior to it being publically available.
4. The controller attempts to upload the information to a SharePoint container against policy.
5. CA DataMinder Endpoint takes into account, location, role and content and determines the post is against policy and action should be blocked to mitigate risk to the business.

Figure B.

Use case 1 (create) - CA DataMinder alerting user of blocked post.

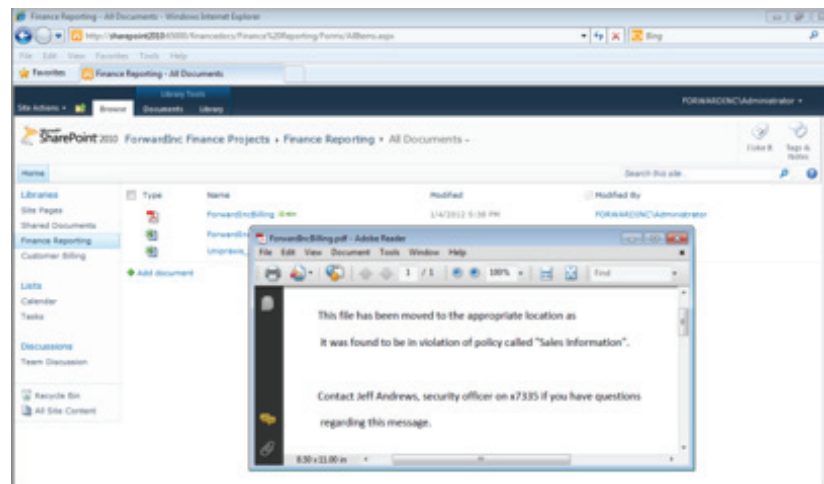


The following depicts how CA DataMinder moves sensitive information to the proper location:

1. A user saves sensitive sales and billing content to a financial reporting folder.
2. CA DataMinder Stored Data classifies the content as customer billing information.
3. CA DataMinder Stored Data determines based on pre-defined policy that the file should be stored within the Customer Billing folder.
4. CA DataMinder moves the file to the billing folder leaving a file stub alerting users that the file has been moved.

Figure C.

Use case 2 (store) - CA DataMinder moves sensitive files.

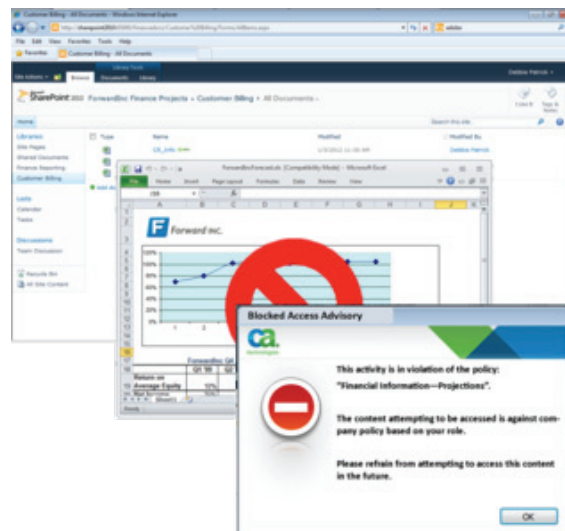


The following depicts how CA SiteMinder with CA DataMinder Classification blocks access to content:

1. An accounts receivable user attempts to access sensitive corporate financial forecast information inappropriately stored within a SharePoint customer billing container.
2. CA SiteMinder integrates with CA DataMinder Classification enabling real-time visibility into the sensitivity of the financial forecast file attempting to be accessed.
3. Since the role of the user accessing this type of content is against policy CA SiteMinder blocks access to the file.

Figure D.

Use case 3 (use) – CA SiteMinder blocks access to sensitive content.

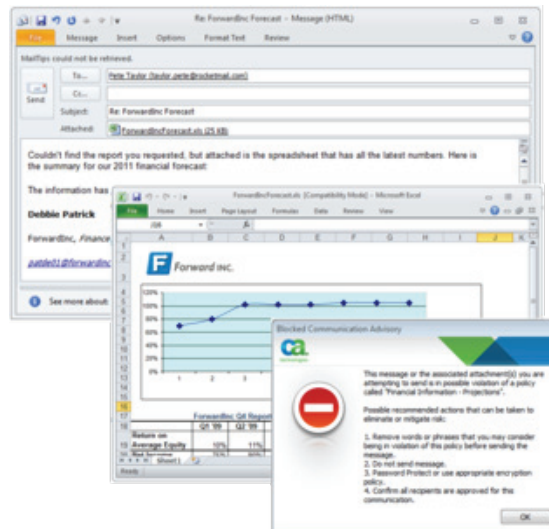


The following depicts how CA DataMinder blocks sensitive information sent over email:

1. As users finalize collaboration and the document is complete, it is considered ready for distribution.
2. But since the document contains sensitive content it is very important only the appropriate recipients receive it.
3. CA DataMinder is able to control the distribution of this document over various modes of communication including uploading it to a social media site, saving to removable media, printing or emailing based on identity and content.
4. CA DataMinder determines the content and mode of communication is against policy and blocks the email.

Figure E.

Use case 4 (distribute) – CA DataMinder controls communication of content.

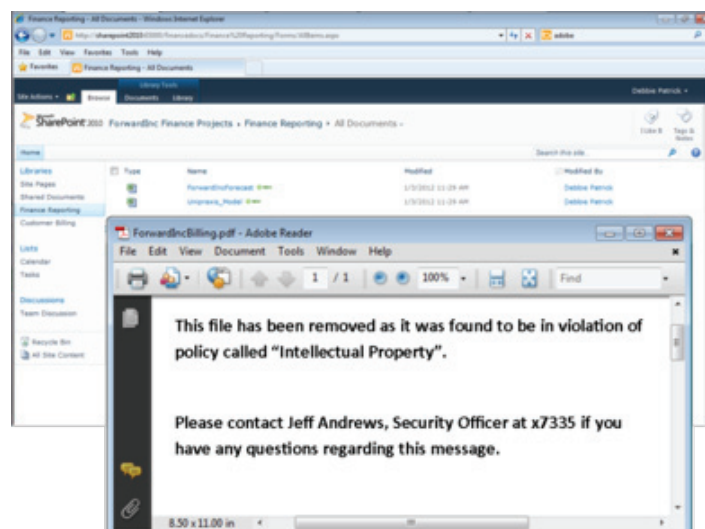


The following depicts how CA DataMinder removes or deletes content from SharePoint:

1. There are levels of content sensitivity not meant for the confines of SharePoint.
2. CA DataMinder Stored Data is able to discover and classify content enforcing policies that don't allow certain content sensitivity levels to be stored within a SharePoint site.
3. For files that do not belong in those locations, CA DataMinder Stored Data is able to replace them with files containing explanations for why they were replaced, and who to contact with questions.
4. Additionally, the original files could be quarantined or moved to a secure location.

Figure F.

Use case 5 (dispose) – CA DataMinder removes content from Sharepoint.



Section 4: Benefits

Benefits of CA Information Lifecycle Control for SharePoint

As sensitive information proliferates within and outside SharePoint sites organizations are opening themselves up to a significant level of financial exposure. In order to protect their core assets they must take a layered approach to reducing their overall level of risk. CA DataMinder enables this by controlling sensitive information throughout the SharePoint Information Lifecycle. This comprehensive approach to information control extends the following benefits.

Measure information risk through discovery and classification

The lack of visibility into the location and sensitivity of SharePoint information is a significant organizational challenge to understanding business impact given the dynamic nature of enterprise data. CA DataMinder is able to help solve this challenge through its ability to automatically discover and classify sensitive content as it's posted, stored and distributed in and out of SharePoint. What previously was a time and resource intensive effort resulting in imperfect information is now a streamlined and consistent process that enables the business to actively understand critical risks to their organization.

Enable business processes while protecting sensitive content

A major goal of IT and security is to deliver a strong balance of business enablement with content protection. The ability to post, share, collaborate and store information within SharePoint enhances business efficiency but also exposes organizations to a significant amount of risk. Organizations must take a layered but precise approach to securing information within SharePoint if they wish to enable the business but mitigate the impact of these threat vectors. CA DataMinder is able to assist organizations in meeting these goals by incorporating identity and content into how sensitive data is controlled throughout the SharePoint Information Lifecycle. This precise but layered approach protects organizations as information is created, stored, used, distributed and disposed of within SharePoint environments. Organizations can now enable the right user to have the right access to the right content.

Reduced risk of information compromise and non-compliance

The sensitivity of information stored within SharePoint can vary widely based on industry, business and functional group. Corporate and regulatory data policies are designed to protect the organization and its customers in regards to the data that is handled. Financial, employee behavior, customer treatment, intellectual property and personally identifiable information are all relevant data types that must be classified and effectively controlled in order to reduce the risk of data compromise and regulatory non-compliance. CA DataMinder is able to discover, classify and protect sensitive information based on pre-defined regulatory and corporate policies in order to help protect the brand and reduce the risk of data compromise and non-compliance.

Section 5: The CA Technologies advantage

CA Content-Aware IAM enables you to not only control user identities and access but information usage. Effective information protection and control is imperative to meeting both corporate compliance requirements and security polices while also enabling critical business processes.

CA Technologies has been a leader in IT management for over 30 years, has over 1000 security customers, and is committed to continuing to bring innovative security capabilities to the marketplace. We have a large and dedicated group of security experts who know how to make security deployments successful, and to help our customers achieve accelerated time-to-value.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.